Part V System Administrator's Guide "B": Community-Supported Implementations

Chapter 21: *Installing Kerberos on a non-Fermi-Supported Linux System*

In this chapter we discuss Kerberizing a machine running a Linux OS other than FRHL, using the Fermi Kerberos source code from the MIT Kerberos product. The instructions provided here should help non-UPS/UPD Linux users achieve a fully-functional Fermilab Kerberos implementation.

Chapter 22: *Installing MIT Kerberos on Windows, for use with Exceed 7 and FileZilla*

In this chapter we describe how to install and configure the MIT Kerberos software to Kerberize your Hummingbird Exceed 7.0 telnet connections on your Windows system (Win2k, NT4, 95, or 98). The MIT Kerberos software for Windows systems comes with a GUI configuration interface called **Leash32**. Installation of the Kerberos software will allow you to connect to Kerberized machines and encrypt your data transmissions.

Chapter 23: *Installing Heimdal Kerberos for use with Cygwin*

In this chapter we get you started installing the Heimdal Kerberos software in order to Kerberize your network connections from a Windows Cygwin system (Win2k or NT4, or other OS running NTFS). Currently, MIT Kerberos and Fermi Kerberos do not run on Cygwin without tweaking and recompiling. Installation of the Heimdal Kerberos software will allow you to connect to Kerberized machines and encrypt your data transmissions.

Chapter 24: *Installing and Configuring MIT Kerberos on a Macintosh System*

In this chapter we describe how to install and configure the **MIT Kerberos for Macintosh 3.5** software on your Macintosh system in order to access Kerberized machines and encrypt your data transmissions.

Chapter 21: Installing Kerberos on a non-Fermi-Supported Linux System

In this chapter we discuss Kerberizing a machine running a Linux OS other than FRHL, using the Fermi Kerberos source code from the MIT Kerberos product[1]. The instructions provided here should help non-UPS/UPD Linux users achieve a fully-functional Fermilab Kerberos implementation.

☞ The Computing Division does not support these types of installations explicitly, but you can request help on the *kerberos-users@fnal.gov* mailing list (and usually obtain it!).

21.1 Before You Install Kerberos

21.1.1 Obtain a Kerberos Principal

Strictly speaking, you don't need a Kerberos principal to just install the software. It will be difficult to judge your results without one, however. You'll need to get one (plus an initial password) to have access to the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal* for information, and fill out the online form at `http://www.fnal.gov/cd/forms/strongauth.html`.

21.1.2 Do you Need to Allow Incoming Kerberos Connections?

For any machine on which services will be offered and which therefore must allow incoming Kerberos connections (including portal mode connections) you must get a service principal for the host, and one for **FTP** if that is an offered service. These service principal names are of the form `host/<full.node.name>` and `ftp/<full.node.name>` (e.g.,

[1] Kerberos V5 is available from other sources as well, and these instructions should work for the general case, except of course for MIT-specific comments.

`host/mynode.fnal.gov` and `ftp/mynode.fnal.gov`, or something like `host/mynode.myuniv.edu` and `ftp/mynode.myuniv.edu`, depending on your institution's domain).

Before installing **kerberos** on a machine the first time, request these host-specific service principals (plus initial passwords) for that machine, using the form at `http://www.fnal.gov/cd/forms/strongauth.html`. You will need to provide the full hostname of the machine.

☞ Notes:

- For a machine with two or more active (static) IP addresses or multiple node names, see section 16.12 *Multiple IP Addresses or Node Names*.
- If you are reinstalling **kerberos** on a machine, you should keep the same host and **FTP** principals. If the `krb5.keytab` is not lost, there's nothing you have to do for these principals. If it is lost, contact *compdiv@fnal.gov* to get password resets on the principals.

If you don't intend to allow incoming connections, don't request these service principals, and just answer "no" when asked if you have the passwords for them during installation of the **kerberos** product. You can request and install them at a later date, if needed (see section 16.10 *Installing Service Host Keys*).

21.1.3 Create an Account that Matches your Principal

We strongly recommend that you create an account/login name on the machine that matches the "primary" (the username part) of your user principal. See section C.2 *If your Principal and Login Name do not Match* under section Appendix C: *More about Choosing a Principal Name*. Note that even if your login name and principal don't match you can still get into your machine (console) after it's Kerberized, as long as your UNIX password is there.

21.1.4 Synchronize your Machine with Time Server

When using Kerberos, the client and server must be time-synchronized with each other, each in its local time zone. A wrong system clock is the single most common authentication problem (it typically appears as a "preauthentication failed" message). Kerberos is configured to allow a discrepancy of about five minutes. **xntp** is a product that you can install on your machine to maintain the system time in agreement with Internet standard time servers. It is available from *fnkits* for some platforms.

If your system runs AFS, don't install **xntp** or any other synchronizing software; AFS does its own synchronization. But beware: AFS doesn't set the hardware clock, so, for example, when daylight savings time starts or ends, your clock may be an hour off. Choose ONLY ONE of the following solutions:

- start **xntp**, let it sync the clock, then turn it off
- see if the **afsd** has a **`-nosettime`** option; if so, set it and run **xntp** to handle the timekeeping instead
- (Linux) make sure the date is correct, then run **`/sbin/hwclock --systohc`** to change the hardware clock to match the system clock (or edit your `crontab` to run the above command at some frequency; e.g., to sync it up once a month, add the line `33 3 3 * * /sbin/hwclock --systohc`)

21.2 Installing MIT Kerberos

1) Bring up the **MIT Kerberos** web page, at URL `http://web.mit.edu/kerberos/www/`. Select Kerberos V5 Release 1.2.

2) Follow the links to the MIT Kerberos Distribution page. You'll need to download the Kerberos source. Scroll down to Kerberos V5 Release 1.2 Source Distributions, and download `krb5-1.2.2.tar.gz, 5240k`.

3) Login as *root*.

4) Unzip and untar the file, creating the directory `krb5-1.2.2`

5) In the `krb5-1.2.2` directory, run `./configure` (use all defaults).

6) Still in `krb5-1.2.2`, run **`make`** and **`make install`**. Now, the software is configured, compiled and installed.

7) Get the latest `krb5.conf` file from Fermi KITS (as of 5/15/01, available as `ftp://ftp.fnal.gov/KITS/GENERIC_UNIX/krb5conf/v1_4/`). The `krb5.conf.template` file from the krb5conf product now has lines containing xMYREALMx and xMYNODEx which have to be edited. To join the production realm, change xMYREALMx to FNAL.GOV and xMYNODEx to the fully-qualified name of host. At this point, you should be able to authenticate to the Fermilab strengthened realm from your machine.

8) In the `/etc/inetd.conf` file, disable the default FTP, telnet, rlogin[1], etc., on your machine, and enable the Kerberized versions. Also comment out or delete the lines starting with "shell", "login", "rexec"

[1] Note that klogind replaces rlogind, and kshd repalaces rshd.

and insert new lines for kshell, klogin and eklogin:

```
## ftp  stream  tcp   nowait  root   /usr/local/sbin/ftpd    ftpd -a
ftp     stream  tcp   nowait  root   /usr/krb5/sbin/ftpd    ftpd -aOP
...
kshell  stream  tcp     nowait  root    /usr/krb5/sbin/kshd kshd -5c
klogin  stream  tcp     nowait  root    /usr/krb5/sbin/klogind klogind -5c
eklogin stream  tcp     nowait  root    /usr/krb5/sbin/klogind klogind -5ce
```

9) Run **`kadmin`**, and use **`ktadd`** to add host and FTP principals to the `/etc/krb5.keytab` file. Run **`kadmin`** as follows (supplying host and FTP passwords as needed):

```
% /usr/krb5/sbin/kadmin -p host/hostname.domain \
  -q “ktadd host/hostname.domain”
% /usr/krb5/sbin/kadmin -p ftp/hostname.domain \
  -q “ktadd ftp/hostname.domain”
kadmin: ktadd host/hostname.domain
kadmin: ktadd ftp/hostname.domain
```

At this point, you can FTP and telnet *into* your machine, as well as *from* it. Now, it’s time to replace the default login program with the Kerberized version. The typical RedHat login program is PAM-aware, but there is no PAM support in MIT Kerberos v1.2.2. In the RH Linux login file (`/etc/pam.d/login`) there is a line:

```
session    optional    /lib/security/pam_console.so
```

The `pam_console.so` module is responsible for changing the ownership and permissions on the console devices. We recommend that you modify the source for the Kerberos `login.krb5` program, `krb5-1.2.2/src/appl/bsd/login.c`, to be PAM-aware.

10) To do this, **`cd`** to the the `krb5-1.2.2/src/appl/bsd/` directory, make a copy of `login.c` (to be safe!), copy the patch shown below into a file in this directory (we call it `patchfile`), and run it:

```
% patch -p0 < patchfile
```

Now the MIT Kerberos `login.c` will call the `pam_console.so` that came with RH Linux.

11) To link to the `pam` and `pam_misc` libraries, modify the Makefile in `krb5-1.2.2/src/appl/bsd`. Replace

```
LOGINLIBS =
```

with

```
LOGINLIBS = -lpam -lpam_misc
```

The Patch

```
--- login.c.origTue Mar  6 15:13:27 2001
+++ login.cWed Mar  7 15:44:56 2001
@@ -81,6 +81,10 @@

 #include <libpty.h>

+/* begin pam stuff */
+#include <security/pam_appl.h>
+#include <security/pam_misc.h>
+/* end pam stuff */
 #ifdef HAVE_UNISTD_H
 #include <unistd.h>
 #endif
@@ -1004,6 +1008,11 @@
     }
 }

+/* begin pam stuff */
+  int retcode;
+  pam_handle_t *pamh = NULL;
+  struct pam_conv conv = { misc_conv, NULL };
+/* end pam stuff */
 int main(argc, argv)
      int argc;
      char **argv;
@@ -1438,6 +1447,11 @@
     quietlog = access(HUSHLOGIN, F_OK) == 0;
     dolastlog(quietlog, tty);

+/* begin pam stuff */
+    retcode  =  pam_start("login.krb5",  username,  &conv,
&pamh);
+  pam_set_item(pamh, PAM_TTY, tty);
+  pam_open_session(pamh, PAM_SILENT);
+/* end pam stuff */
     if (!hflag && !rflag && !kflag && !Kflag && !eflag) {/*
XXX */
 static struct winsize win = { 0, 0, 0, 0 };

@@ -2394,6 +2408,10 @@
 #ifdef _IBMR2
     update_ref_count(-1);
 #endif
+/* begin pam stuff */
+   pam_close_session(pamh, PAM_SILENT);
+   pam_end(pamh, PAM_SUCCESS);
+/* end pam stuff */
```

This patch only enables the session module-type. If you add auth, account and/or password module-types, you may compromise the Kerberos security.

21.3 Installing Fermi Kerberos

21.3.1 Download Modified Source from CVS

Instead of installing non-Fermi Kerberos software and enabling the locally-added features of Kerberos, you can download the modified source from the Computing Division CVS repository:

```
% cvs -d :pserver:kpilot@cdcvs.fnal.gov:/cvs/cd co kerberos
```

Read (and be sure you understand!) the `README.*` files in the `ups/` directory. Then configure, compile and install.

21.3.2 Download Tar File from KITS

If you're running a Fermi-supported OS but not UPS/UPD, you can fetch the **kerberos** product tar file from fnkits.fnal.gov, untar it into `/usr/krb5`, then carry out the `/etc/services`, `/etc/inetd.conf` and `/etc/krb5.keytab` steps by hand, and get the `krb5.conf` file from the **krb5conf** product or from another system.

Assuming that you're logged on as *root* and `/usr/krb5/sbin` is in your PATH, the command to do the keytab file is:

```
kadmin -q "ktadd host/<node>.fnal.gov" -p host/<node>.fnal.gov

kadmin -q "ktadd ftp/<node>.fnal.gov" -p ftp/<node>.fnal.gov
```

and provide the passwords.

Chapter 22: Installing MIT Kerberos on Windows, for use with Exceed 7 and FileZilla

In this chapter we describe how to install and configure the MIT Kerberos software on your Windows system (Win2k, NT4, 95, or 98). This software, when used with the Hummingbird Exceed 7.0 telnet client and the FileZilla FTP client, allows you to authenticate to Kerberos, open Kerberized connections to remote machines, and encrypt your data transmissions. The MIT Kerberos software for Windows systems comes with a GUI called **Leash32**.

☞ Note that while the configuration described in this chapter complies with the Fermilab Policy on Computing and some divisions are recommending and supporting it, it is not formally supported by the Computing Division.

22.1 Getting Ready

22.1.1 Obtain a Kerberos Principal

First, verify that you have administrator privileges on the PC. Next, you need to obtain a Kerberos principal and initial password for the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal*.

22.1.2 Install Exceed and FileZilla

Exceed 7.0[1]

Exceed is a licensed product. We do not describe the installation process in this document. Versions prior to 7 do not support Kerberos. Version 7.0.0.0 must be patched, since it has a number of severe bugs. You can check the

[1] The Exceed version information presented here was taken from the Beams Division documentation at `http://www-bdnew.fnal.gov/network/latest-software-versions.htm`.

Exceed version number by starting Exceed. The startup screen shows 7.0.0.0 for unpatched systems. The correct version shows 7.0.0.12 when starting Exceed, and 7.0.0.5 when starting Exceed host explorer.

Hummingbird Exceed 7.0 FTP connections cannot be Kerberized.

FileZilla 1.93

FileZilla is a small (791k) but powerful freeware FTP client that supports Kerberos (as well as firewalls and proxy connections). It claims to work on virtually all the Windows platforms: W2k/NT/9x/ME/XP. The software includes a site manager to store all your connection details and logins as well as an Explorer-style interface that shows the local and remote folders and can be customized independently. Additional features include keep alive and auto ascii/binary transfer.

Download the software from `\\Pckits\PC_Tools\Apps\FileZilla_1.6\FileZilla_1_6setup.exe`. Instructions are provided in the same directory. We do not describe the installation process in this document. However, we want to draw your attention to a couple of configuration issues. Under **EDIT > SETTINGS > CONNECTION >**

- **GSS SUPPORT**: Check `Enable Kerberos GSS support`, and add `FNAL.GOV` to the **GSS ENABLED SERVERS** list (you can remove `mit.edu`).
- **FIREWALL SETTINGS**: Check `Passive Mode`

22.1.3 Caveats

Although it appears that you can use **Leash32** to configure Kerberos for multiple realms, we have only gotten this software to work reliably when configured for accessing a single realm.

As mentioned above, Hummingbird Exceed 7.0 FTP connections cannot be Kerberized; use FileZilla’s FTP client.

22.2 Installing Kerberos

1) Log into an account with administrator privileges.

2) Download the Kerberos client software from MIT. First browse to: `http://web.mit.edu/network/kerberos-form.html`.

This brings you to the **Kerberos Distribution Authorization Form**. Answer the three questions, and submit the form to arrive at the download page, **Welcome to the MIT Kerberos Distribution Page!**. Scroll down (about half-way) to the section on *MIT Kerberos for Windows 2.1* and click on the file listed next to KfW 2.1 Installer (it is currently called `kfw-2.1-installer.exe`). Save the file to disk. The default location it chooses is `C:\Program Files\Accessories`.

3) Once this file is copied on to your machine, execute it to install the Kerberos program. You will be asked a series of questions, but you can safely use the defaults, and just click through the screens. Checking the time synchronization when prompted is a good idea. The software gets installed under `C:\Program Files\Kerberos` by default.

4) After installing the files, it will ask if it's OK to restart your computer. Say yes.

22.3 Configuring Kerberos using Leash32

1) Log back on to the same account.

2) Create the configuration file `krb5.ini` as listed in section 22.6 *krb5.ini for FNAL.GOV*, and put it in your Kerberos folder. (If you accepted the default installation values, this folder is under `C:\Program Files`.) The `krb5.ini` file is comparable to the `krb5.conf` on UNIX.

3) Find where **Exceed 7** has installed the file `krbv4w32.dll` (should be the Kerberos folder), and delete this file.

4) Navigate to **START** > **PROGRAMS** > **KERBEROS UTILITIES** > **LEASH32**. (**Leash32** is a GUI for your Kerberos client.)

5) On the **LEASH32** window, go to the **OPTIONS** menu and select **KERBEROS PROPERTIES**.

6) Under **TICKET LIFETIME**, choose how long you would like your tickets to last (in minutes). 1500 is a good choice. The rest of the configuration under this heading is done for you.

7) Back on the **LEASH32** window, go to the **OPTIONS** menu and select **KERBEROS V5 PROPERTIES**. Under the *Configuration Options* tab, check **FORWARDABLE** to make your Kerberos tickets forwardable to remote Kerberized hosts. Under the *File Location* tab, check that the configuration file path is correct.

8) Also on the **OPTIONS** menu, select **DESTROY TICKETS/TOKENS ON EXIT**.

22.4 Getting a Ticket

To authenticate locally using the **Leash32** utility, select **GET TICKET(S)** on the **ACTION** menu. You will be required to enter your Kerberos password. Ignore the CRYPTOCard prompt that may follow (press **CANCEL**). You ticket will appear in the **Leash32** window. Click on the Windows Explorer-style plus signs (+) to get details.

Alternatively, you can invoke the command prompt and type **`kinit -5`** to request a ticket. You will be required to enter your Kerberos password. Ignore the CRYPTOCard prompt that may follow (just press **ENTER**). To verify the ticket and its flags, either bring up the **Leash32** window, or type **`klist -f`** at the command prompt.

22.5 Configuring the Exceed 7 Telnet Application

22.5.1 Create a new Telnet Profile for Kerberized Host

You should create one profile for each Kerberized host you wish to access.

1) Start the Exceed 7 telnet program. Navigate to **START** > **PROGRAMS** > **HUMMINGBIRD CONNECTIVITY V7.0** > **HOSTEXPLORER** > **TELNET**.

2) In the **OPEN SESSION** window, click on the icon in the upper right corner (second from right) that has the blue screen inside the box with the yellow stripe over it (Rollover text is: `Create New Profile`). Set the following values:

   a) Profile Name = any name to identify the profile (e.g., target host name)

   b) Profile Type = VT

   c) Connect by = Telnet

   d) Hostname = the fully qualified name or IP address of name of the target host (e.g., myhost.fnal.gov or 131.225.876.54)

3) Back on the **OPEN SESSION** window, right-click on the profile you just created and select **PROPERTIES**.

4) In the **SETTINGS GROUP** area of the session profile, expand the **SECURITY** folder, and select **KERBEROS**.

   a) Change the **KERBEROS VERSION** to Kerberos 5 from the pulldown menu.

   b) In the **COMMON KERBEROS OPTIONS** field, check both Authentication and Encryption.

   c) In the **KERBEROS 5 OPTIONS**, check Forwarding. If your user name on the target machine is different from your principal, enter your user name under Alternate User Name.

   d) Click **OK**.

22.5.2 Create a new Telnet Profile for nonKerberized Host

You should create one profile for each host you wish to access.

1) Start the Exceed 7 telnet program. Navigate to **START** > **PROGRAMS** > **HUMMINGBIRD CONNECTIVITY V7.0** > **HOSTEXPLORER** > **TELNET**.

2) In the **OPEN SESSION** window, click on the icon in the upper right corner (second from right) that has the blue screen inside the box with the yellow stripe over it (Rollover text is: `Create New Profile`). Set the following values:

   a) Profile Name = any name to identify the profile (e.g., target host name)

   b) Profile Type = VT

   c) Connect by = Telnet

   d) Hostname = the fully qualified name or IP address of name of the target host (e.g., myhost.fnal.gov or 131.225.876.54)

   e) Click **OK**.

22.5.3 Connect to Kerberized Host using Telnet Profile

1) On the **OPEN SESSION** window, with your new profile selected, the target host name or IP address should appear in the Host Name window. To connect, click on the **CONNECT** button. If you’ve preauthenticated,

you should get right in without having to provide your Kerberos password.

2) The **LEASH32** window should now show your host connection in addition to the kerberos ticket.

22.5.4 Connect to nonKerberized Host using Telnet Profile

On the **OPEN SESSION** window, with a nonKerberized profile selected, the target host name or IP address should appear in the Host Name window. To connect, click on the **CONNECT** button. You will need to log in normally.

22.6 krb5.ini for FNAL.GOV

Make sure you have tabs in front of the items in each stanza, not a series of spaces.

```
[domain_realm]

        fnal.gov = FNAL.GOV



[libdefaults]

        default_realm = FNAL.GOV

        default_tgs_enctypes = des-cbc-crc

        default_tkt_enctypes = des-cbc-crc

        forwardable = true

        proxiable = true



[login]

        krb4_convert = true

        krb4_get_tickets = true
```

```
[realms]

        FNAL.GOV = {
                kdc = krb-fnal-1.fnal.gov:88
                kdc = i-krb-7.fnal.gov:88
                kdc = krb-fnal-2.fnal.gov:88
                kdc = krb-fnal-3.fnal.gov:88
                kdc = krb-fnal-4.fnal.gov:88
                kdc = krb-fnal-5.fnal.gov:88
                admin_server = krb-fnal-admin.fnal.gov
                default_domain = fnal.gov        }
```

Chapter 23: Installing Heimdal Kerberos for use with Cygwin

In this chapter we get you started installing the Heimdal Kerberos software in order to Kerberize your network connections from a Windows Cygwin system (Win2k or NT4, or other OS running NTFS). Currently, MIT Kerberos and Fermi Kerberos do not run on Cygwin without tweaking and recompiling. Installation of the Heimdal Kerberos software will allow you to connect to Kerberized machines and encrypt your data transmissions.

☞ Notes:

- While the configuration described in this chapter complies with the Fermilab Policy on Computing and thus may be used, it is not supported at Fermilab.
- The documentation we are providing on this configuration is cursory.
- Work is being done on getting Fermi **kerberos** to compile under Cygwin. Stay tuned...
- Testing of Heimdal has been minimal.
- The Heimdal distribution includes Kerberized daemons that can be used for Kerberizing a Windows machine. However we restrict our discussion to setting the machine up as a Kerberos client only.

23.1 Obtain a Kerberos Principal

First, verify that you have administrator privileges on the PC. Next, you need to obtain a Kerberos principal and initial password for the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal*.

23.2 Install Cygwin

Cygwin runs on Win2K, and on NT using NTFS. This discussion is based on a Win2K install. The full Cygwin installation requires ~ 300 MB of space. This can be reduced by selecting only the tools desired from the installation.

23.2.1 Partial Installation

In order to run the Heimdal kerberos client software, you don't need to install the full Cygwin. The minimum installation for Kerberized telnet and ftp for Windows can be accomplished by downloading six files, all available for download from the URL `ftp://ftp.it.su.se/pub/kerberos/contrib/win32/`. The six necessary files are:

- `cygwin1.dll` (the DLL file necessary to run Cygwin executables under Windows)
- `telnet.exe`
- `rsh.exe`
- `ftp.exe`
- `kinit.exe`
- `kdestroy.exe`

The four executables and the DLL can be put into `C:\WINNT\SYSTEM32`[1] or into a directory of your choice, provided that the client executables can find the DLL file. We recommend that you copy the DLL file to one of the following locations: the same directory as the executables, `C:\WINNT\SYSTEM32`, or to some other directory in the PATH. If you choose a different location, make sure the directory containing the DLL is in your PATH[2] before you try running the programs.

23.2.2 Complete Installation

Cygwin can be installed from: `http://sources.redhat.com/cygwin/`. There is an icon on the upper right of this page that is titled **INSTALL CYGWIN NOW**. Click this icon to download the `setup.exe` program to your hard drive.

Run the `setup.exe` program to begin installation (Sorry, no screen-by-screen details!).

[1] Assuming that `%SYSTEMROOT%` is `C:\WINNT`.

[2] To get to the PATH, navigate to **START > SETTINGS > CONTROL PANEL > SYSTEM > ENVIRONMENT**.

23.3 Install Heimdal Kerberos

The Heimdal distribution of kerberos is available via a binary distribution at: `ftp://ftp.it.su.se/pub/kerberos/contrib/win32/`. The file of interest is `travelkit.zip`. This binary distribution is based on the Heimdal 0.3e source. The current source is 0.4b and is available via a link from the Heimdal page `http://www.pdc.kth.se/heimdal/`. (If you prefer to compile the current source under Cygwin, which requires some tweaking of the source, send a request to *kerberos-users@fnal.gov*.)

To install the `travelkit.zip`:

- Expand the zip file into the `/usr` directory (under Cygwin `/usr` becomes `//c/cygwin/usr`).

  This will populate the `/usr/heimdal` directory as well as drop a sample `krb5.conf` file in the `/usr/etc` directory.
- Remove the sample `krb5.conf` file.
- Obtain a standard Fermi `krb5.conf` (available from KITS as the product **krb5conf**, or just copy from a Kerberized UNIX machine), and copy it to the `/etc` directory.
- Put the `/usr/heimdal/bin` directory in your PATH.

In the `/usr/heimdal/bin` directory you will find the available client tools. There are Kerberized clients for telnet, FTP, rsh and rcp (rlogin is not yet available).

23.4 Using CVS under Cygwin

The Heimdal Kerberized **rsh** allows the Cygwin CVS client to work with Kerberos authentication. Put the Kerberized rsh in your $PATH, and set your CVSROOT variable to the appropriate value, e.g., `cvsuser@cdcvs.fnal.gov:/cvs/cd`. Authenticate to Kerberos, and then, for example, you can execute **`cvs co kerberos`** to get the kerberos source.

Chapter 24: Installing and Configuring MIT Kerberos on a Macintosh System

In this chapter we describe how to install and configure the **MIT Kerberos for Macintosh 4.0x** software[1] on your Macintosh system in order to access Kerberized machines and encrypt your data transmissions.

Computing Division Macintosh Strategy

The Computing Division released a statement in January 2001 regarding the policy on Macintosh support. We quote from it here:

"The Macintosh Operating System is no longer a supported operating system from the Computing Division and is not a strategic operating system for future plans...

... Specifically regarding the Strong Authentication realm, the supported access method from Macintoshes will be via the CRYPTOCard. Kerberos clients may be available and used, but there will be no effort expended to select, test or distribute them."

That said, there is some community support for the Macintosh, primarily through *kerberos-users@fnal.gov*. We also provide information here to assist Macintosh users.

We do not currently have a recommendation for Macintosh users outside of the U.S. and Canada. MIT does not yet interpret U.S. regulations as allowing export, so it is the responsibility of the downloader to be in compliance. MIT's statement on Kerberos export control is maintained at `http://web.mit.edu/kerberos/www/export.html`. The MIT Kerberos software for Macintosh is not made freely available on the `http://www.crypto-publish.org/` web site because it includes code built from non-open sources. You may want to consider upgrading your OS to OS X and using the Kerberos software for UNIX.

[1] Version 4.0a12 has since been made available.

24.1 Installing MIT Kerberos for Macintosh

First, obtain a Kerberos principal and initial password for the FNAL.GOV realm. See section 3.1 *Your Kerberos Principal*.

This section was originally written for version 3.5 of the MIT kerberos software for Macintosh. Various versions 4.0x have since been made available. Installation can be accomplished by clicking on the “Kerberos for Mac 4.0” installer application. This should install everything into the disk containing your System Folder. This version includes the Kerberos Floating Window (for status), and Kerberos Menu on the menubar (a quick way to create/destroy tickets and to open the Kerberos Control Panel). You will need to reboot probably twice, then, assuming your Kerberos Preferences file is configured properly, you should successfully get a ticket for your principal.

Note that MIT Kerberos for Macintosh was shipped as part of Mac OS X in the OS X 10.1 update shipped by Apple. There is a kit of “extras” for OS X 10.1 with some additions to what was shipped with the OS. See `http://web.mit.edu/macdev/Development/MITKerberos/Common/Documentation/osx-kerberos-extras.html`.

24.1.1 Changes in MIT Kerberos for Macintosh 4.0

See `http://web.mit.edu/macdev/Development/MITKerberos/Common/Documentation/release-4.0.html`. A big change is better OS X support. User interface changes relative to v3.5 include:

- The **KERBEROS CONTROL PANEL** is a changed version of the **KERBEROS MANAGER**.
- The **KERBEROS MENU** on the menu bar shows the status of the active user’s TGT and can be used to quickly get/destroy/renew tickets or open the control panel.
- The **KERBEROS CONTROL STRIP** is similar to the **KERBEROS MENU** but a module in the control strip.
- Kerberos Floating Window
- Optional status display of all user’s TGTs.

Regarding installation, version 4.0 includes two installer programs, one for OS X and the other for OS 8/9 (supports 8.1 through 9.2.1) but is otherwise much the same as version 3.5.

24.1.2 Download Kerberos from the MIT Web Site

1) Bring up the **MIT Kerberos for Macintosh** web page, at URL `http://web.mit.edu/macdev/www/kerberos.html`.

2) Select *Getting MIT Kerberos for Macintosh*.

3) On this page, look for the paragraph that starts "If you are outside of MIT but still in the US or Canada...". Click on the *download page* link in that paragraph.

4) This brings you to the **Kerberos Distribution Authorization Form**. Answer the three questions, and submit the form to arrive at the download page. (There is a link on this page for Canadian users, which we have not tried or documented.)

5) Click on the link for MIT Kerberos for Macintosh 4.

6) Under the small heading "Binaries and SDKs", click *Binhexed self mounting disk image*.

24.1.3 Items that Appear on your Desktop

You'll find three new items on your desktop once the transfer finishes (This section has not been updated since v3.5; you will find similar things for v4.0.):

- `MIT Kerberos for the Mac` folder
- `MIT_Kerberos_for_Mac_3.5.hqx` file
- `MIT Kerberos for Mac 3.5.smi` file

There will also be a new disk volume from mounting the `.smi` (if the disk is not present, double-click the `.smi` file).

Discard the `hqx` file, and open the `MIT Kerberos for the Mac` folder. This folder contains:

- two subfolders:
  - `Mac OS 9 Binaries 3.5`, which contains four sub-subfolders labelled as per their destination folders (the names are of the form `->Into <Foldername>`)
  - `Mac OS 9 SDK 3.5`; this is the software development kit and can be ignored.
- one application program **Kerberos for Mac 3.5**
- three links/HTML files: to the MIT Kerberos home page, to the Kerberos for Macintosh Bugs page, and to the KfM 3.5 Release Notes.
- one text file `KfM 3.5 Read Me`, which contains installation instructions

☞ The Kerberos for Macintosh 4.0 disk will have similar contents with the addition of the "Kerberos for Mac OS X 4.0" application and a link "Mac OS X SDK Information". Note that 4.0 supports both Mac OS 8.1 through 9.1 as well as Mac OS X.

24.1.4 Installation Instructions

(This section has not been updated since v3.5; v4.0 is similiar.) We refer you to the `Read Me` file to complete the installation of `MIT Kerberos for the Mac`, but we provide a few clarifications here:

- On the MIT download page, double-click the `Kerberos for Mac 3.5` application to install.
- The downloaded files no longer need to be copied manually into folders under the `System Folder` on your system.
- The `->Into Preferences` folder contains three subfolders. Choose `Kerberos Preferences v5`.

After installation, if you get the error message “preauthentication fails” when you attempt login via the **GET TICKETS** button, it is most likely caused by a password or time-sync error. First verify your password is correct. Then, synchronize your machine with the network time (follow the instructions at `http://hdstock.mit.edu/answers/102.html`). The Date & Time control panel under OS 8.6 and later allows one to select a Network Time Server. The Apple time server (time.apple.com) can be used.

24.2 Configuring the Kerberos Software

24.2.1 The Preferences File

The `Kerberos Preferences` file needs to contain information for Fermilab’s strengthened realm(s). Edit the file or just replace the initial contents with that of the `krb5.conf` file from either the **krb5conf** product in KITS or a machine in the Fermilab FNAL.GOV realm (note that pasting text directly from a web browser may cause end-of-line problems). A Fermi-configured Preferences file is now available for download from `http://www.fnal.gov/docs/strongauth/ps/` (see `Kerberos_Preferences.sit` for the StuffIt archive file, or `Kerberos_Preferences.hqx` for the BinHexed (ASCII encoding) version of that file). We reproduce the text of the file here:

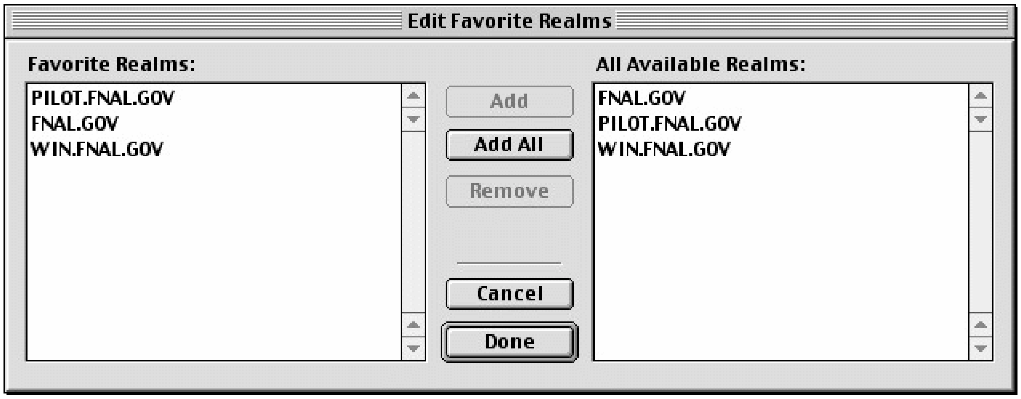
```
[libdefaults]
        default_realm = FNAL.GOV
```

```
         ticket_lifetime =1560
         checksum_type = 1
         ccache_type = 2
         default_tkt_enctypes = des-cbc-crc
         default_tgs_enctypes = des-cbc-crc
         noaddresses = true

[realms]
        FNAL.GOV = {
                kdc = krb-fnal-1.fnal.gov:88
                kdc = krb-fnal-2.fnal.gov:88
                kdc = krb-fnal-3.fnal.gov:88
                kdc = krb-fnal-4.fnal.gov:88
                kdc = krb-fnal-5.fnal.gov:88
                admin_server = krb-fnal-admin.fnal.gov
                default_domain = fnal.gov
                                           auth_to_local   =
RULE:[1:$1@$0](.*@PILOT\.FNAL\.GOV)s/@.*//
                auth_to_local = DEFAULT
        }
        PILOT.FNAL.GOV = {
                kdc = krb-pilot-1.fnal.gov:88
                kdc = krb-pilot-3.fnal.gov:88
                kdc = krb-pilot-4.fnal.gov:88
                kdc = krb-pilot-5.fnal.gov:88
                admin_server = krb-pilot-admin.fnal.gov
                default_domain = fnal.gov
                                           auth_to_local   =
RULE:[1:$1@$0](.*@FNAL\.GOV)s/@.*//
                auth_to_local = DEFAULT
        }
        WIN.FNAL.GOV = {
                kdc = newpckits.fnal.gov:88
                admin_server = newpckits.fnal.gov
                default_domain = fnal.gov
        }

[domain_realm]
        .fnal.gov = FNAL.GOV
        .hep.net = FNAL.GOV
        .minos-soudan.org = FNAL.GOV
```

Note: if you have to deal with Network Address Translation (NAT), see section 5.9.4 *Network Address Translation*.

24.2.2 Select Favorite Realms

After modifying the **KERBEROS PREFERENCES**, start the **KERBEROS CONTROL PANEL** and select the **FAVORITE REALMS** item from the **EDIT** menu. Use the dialog box to copy your favorite realms from the right to the left-hand side of the screen.



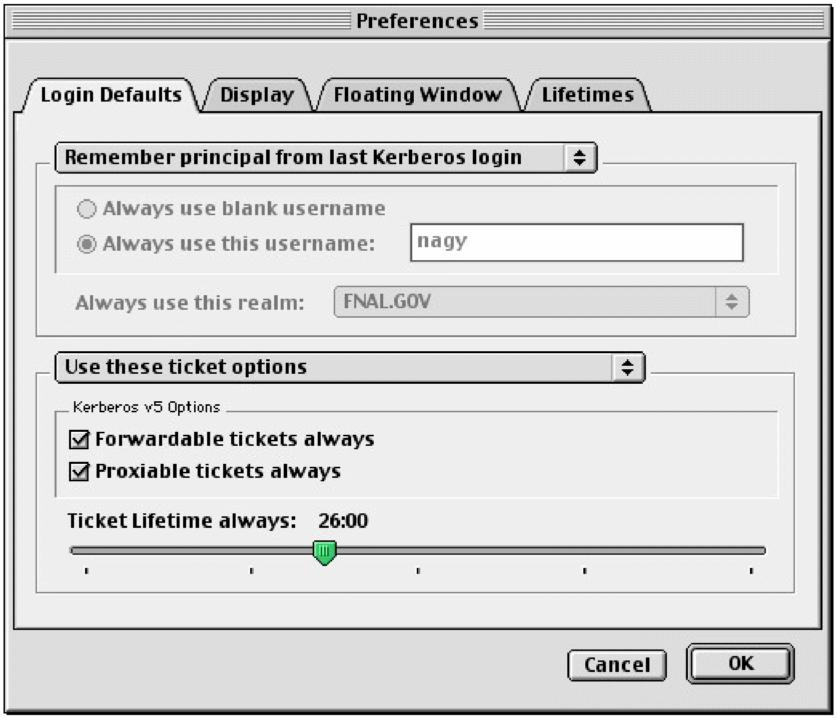
Edit Favorite Realms

Favorite Realms:
PILOT.FNAL.GOV
FNAL.GOV
WIN.FNAL.GOV

All Available Realms:
FNAL.GOV
PILOT.FNAL.GOV
WIN.FNAL.GOV

24.2.3 Edit Preferences

Edit your login preferences, and make sure you check **FORWARDABLE TICKETS ALWAYS**:



Preferences

Remember principal from last Kerberos login

○ Always use blank username
● Always use this username: nagy

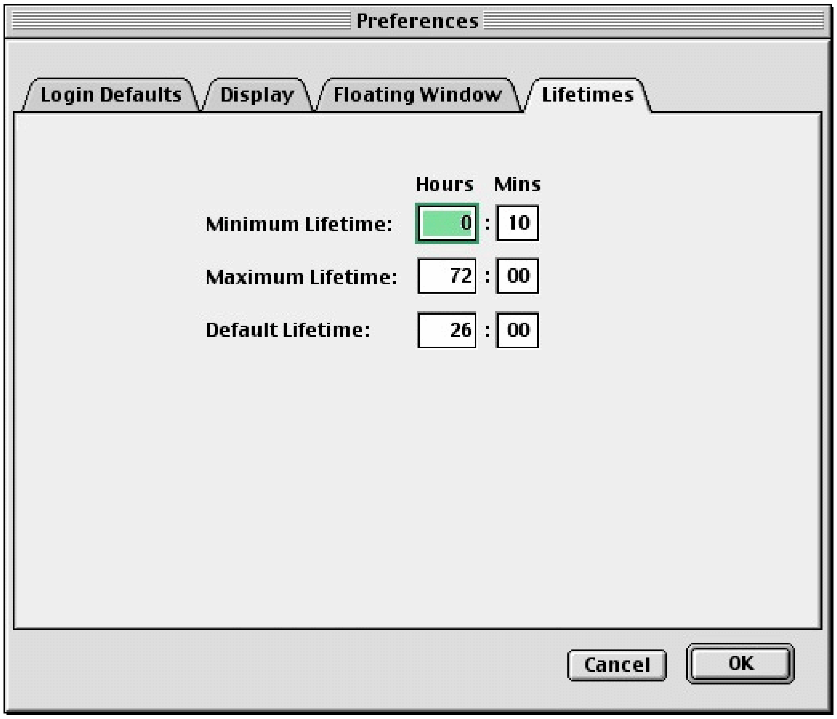
Always use this realm: FNAL.GOV

Use these ticket options

Kerberos v5 Options
☑ Forwardable tickets always
☑ Proxiable tickets always

Ticket Lifetime always: 26:00

Edit your ticket lifetime preferences (the KDC limits the ticket lifetime to 26 hours):



	Hours		Mins
Minimum Lifetime:	0	:	10
Maximum Lifetime:	72	:	00
Default Lifetime:	26	:	00

24.2.4 Edit Favorites

24.3 Installing Telnet Client

BetterTelnet and **NiftyTelnet** with Kerberos v5 support are the only **telnet** products that we know of at this time that work on the Macintosh. We document **BetterTelnet** here. You'll need both it and an associated plug-in installed on your machine.

1) Bring up the **MIT Kerberos for Macintosh** web page, at URL `http://web.mit.edu/macdev/www/kerberos.html`. Select *Frequently Asked Questions*.

2) Look for the Q/A that discusses **telnet** (you can search on "BetterTelnet"). Click on the link *BetterTelnet and Kerberos plugin*. This brings you to the FTP site:

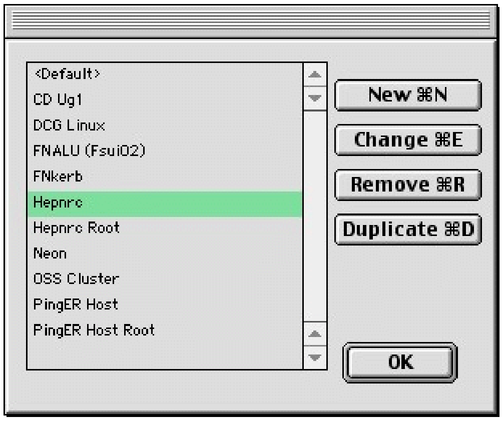
`ftp://ftp.cmf.nrl.navy.mil/pub/chas/MIT_Kerberos_3.5/`.

3) If you don't already have **BetterTelnet** installed, click on `BetterTelnet 2.0f...` and install this software first.

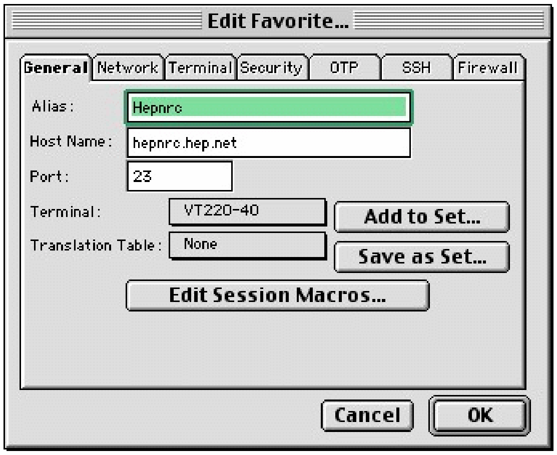
4) Once **BetterTelnet** is installed, download `Telnet_Plugin.bin` from the same **FTP** site and copy it to the **BetterTelnet** folder on your machine.

24.4 Configuring Telnet

1) Invoke **BetterTelnet**. On the **FAVORITES** menu, choose **EDIT FAVORITES**. You should create one configuration for each strengthened host you plan to access.



2) To create a new configuration, on the pop-up screen, click **NEW**. Then, with the **GENERAL** tab selected, type in an **ALIAS** which will be used to identify the host (this can be any string) and the **HOST NAME**.



Alias: Hepnrc

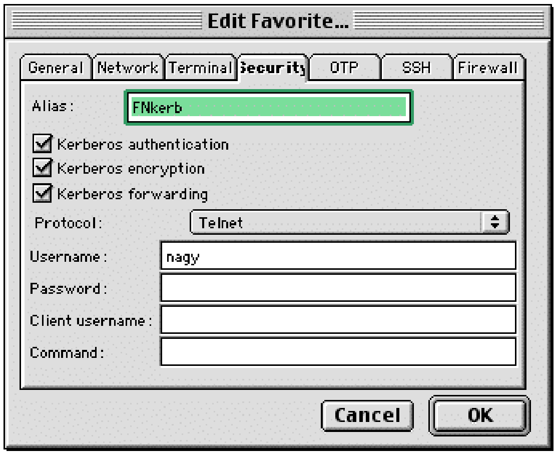
Host Name: hepnrc.hep.net

Port: 23

Terminal: VT220-40

Translation Table: None

☞ 3) **Very important!!** Change to the **SECURITY** tab, check `Kerberos authentication` and `Kerberos encryption`. `Kerberos` `forwarding` is recommended. The protocol should be left as `telnet` (the default). Filling in other fields is optional (even if you fill in your Kerberos password, you need to provide it again when you authenticate). Click **OK** to save the configuration.



Alias: FNkerb

☑ Kerberos authentication

☑ Kerberos encryption

☑ Kerberos forwarding

Protocol: Telnet

Username: nagy

Password:

Client username:

Command:

24.5 Kerberized FTP Client

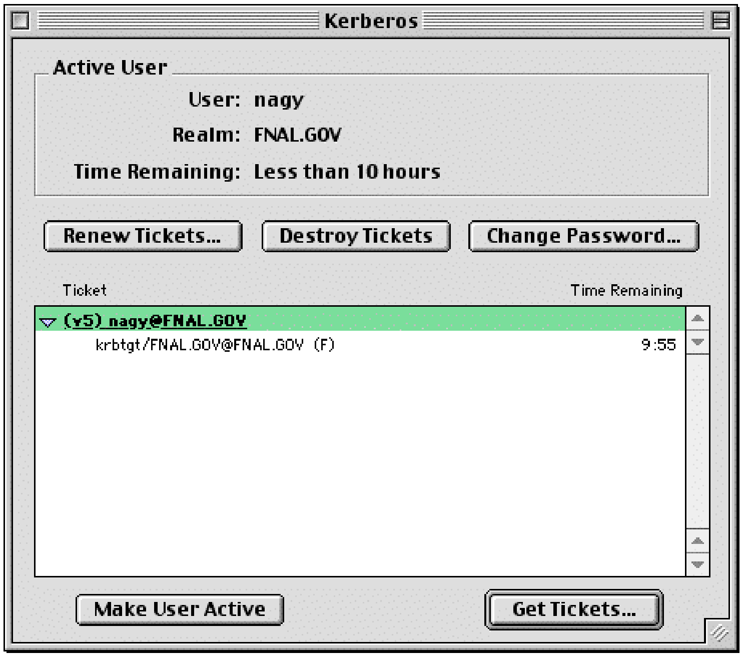
Fetch 3.0.4 beta Secure is freeware for Macintosh. It can be downloaded from the MIT Kerberos Distribution Page at `http://web.mit.edu/network/kerberos-form.html`.

Also, Fetch 4.0 is shareware available from Fetch Softworks at `http://www.fetchsoftworks.com/`. Installation instructions are not provided here (at least not yet!).

24.6 Authenticating to Kerberos

24.6.1 Authenticate via Kerberos Control Panel

- Invoke the **Kerberos Control Panel** (from **CONTROL PANELS** under the Apple menu, from the **KERBEROS MENU** in the menu bar, or from the **KERBEROS CONTROL STRIP** module).



User: nagy

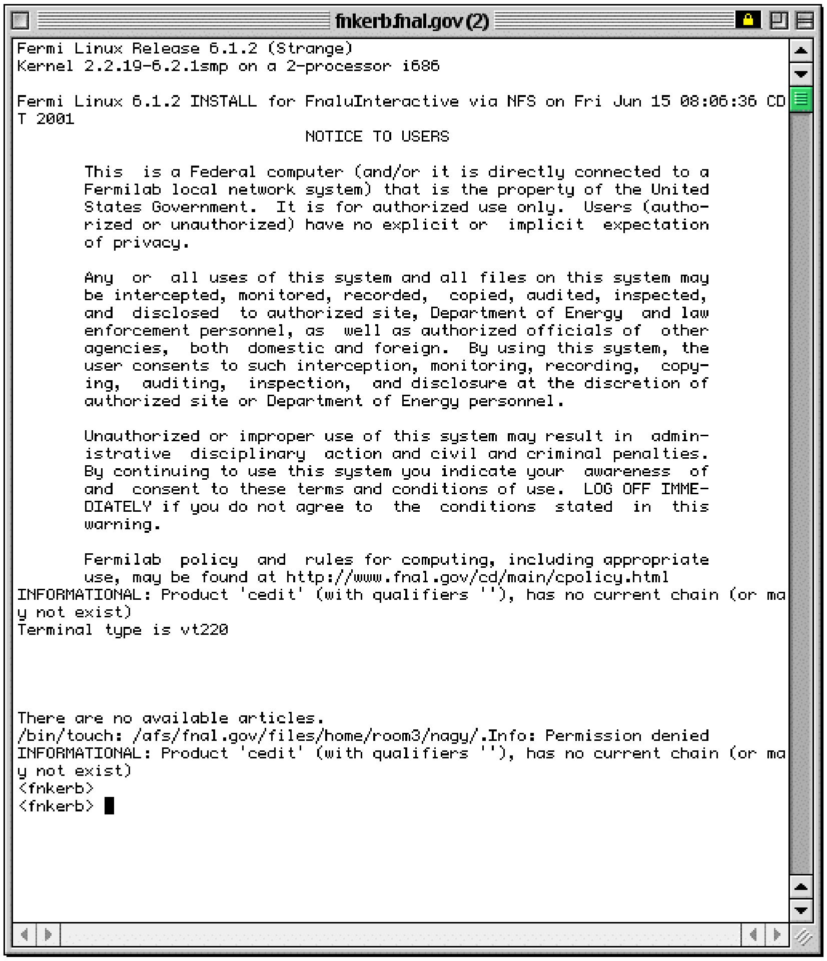
Realm: FNAL.GOV

Time Remaining: Less than 10 hours

```
Ticket                                                Time Remaining
▽ (v5) nagy@FNAL.GOV
     krbtgt/FNAL.GOV@FNAL.GOV (F)                                9:55
```

- Select principal, and click **GET TICKETS**.
- Enter your Kerberos password on the pop-up screen.

You should see a ticket appear. Now you can invoke your **telnet** product (**BetterTelnet** or **NiftyTelnet**) and connect to one or more strengthened hosts without having to provide your password again.



```
Fermi Linux Release 6.1.2 (Strange)
Kernel 2.2.19-6.2.1smp on a 2-processor i686

Fermi Linux 6.1.2 INSTALL for FnaluInteractive via NFS on Fri Jun 15 08:06:36 CD
T 2001
                              NOTICE TO USERS

       This  is a Federal computer (and/or it is directly connected to a
       Fermilab local network system) that is the property of the United
       States Government.  It is for authorized use only.  Users (autho-
       rized or unauthorized) have no explicit or  implicit  expectation
       of privacy.

       Any  or  all uses of this system and all files on this system may
       be intercepted, monitored, recorded,  copied, audited, inspected,
       and  disclosed  to authorized site, Department of Energy  and law
       enforcement personnel, as  well as authorized officials of  other
       agencies,  both  domestic and foreign.  By using this system, the
       user consents to such interception, monitoring, recording,  copy-
       ing,  auditing,  inspection,  and disclosure at the discretion of
       authorized site or Department of Energy personnel.

       Unauthorized or improper use of this system may result in  admin-
       istrative  disciplinary  action and civil and criminal penalties.
       By continuing to use this system you indicate your  awareness  of
       and  consent to these terms and conditions of use.  LOG OFF IMME-
       DIATELY if you do not agree to  the  conditions  stated  in  this
       warning.

       Fermilab  policy  and  rules for computing, including appropriate
       use, may be found at http://www.fnal.gov/cd/main/cpolicy.html
INFORMATIONAL: Product 'cedit' (with qualifiers ''), has no current chain (or ma
y not exist)
Terminal type is vt220




There are no available articles.
/bin/touch: /afs/fnal.gov/files/home/room3/nagy/.Info: Permission denied
INFORMATIONAL: Product 'cedit' (with qualifiers ''), has no current chain (or ma
y not exist)
<fnkerb>
<fnkerb> █
```

24.6.2 Authenticate at Login

Invoke **BetterTelnet** or **NiftyTelnet** and connect to a strengthened host. You will be prompted for your Kerberos password, and then authenticated once you have provided it.